Caso applicato al profilo

AREA dei Collaboratori (ex Area A e As)

LA GESTIONE DELLE RELAZIONI INTERNE ED ESTERNE

La protezione dei dispositivi digitali

ENRICO BASILE

Enrico BASILE è laureato in Scienze Religiose presso la Facoltà Teologica dell'Italia Settentrionale – sezione di Torino. Ha maturato una vasta esperienza nell'ambito della gestione amministrativo-contabile delle istituzioni scolastiche, ricoprendo incarichi di DSGA anche in contesti complessi e su più sedi.

Ha intrapreso un percorso accademico e formativo trasversale, comprendente anche studi economici e giuridici, con particolare attenzione alla normativa scolastica, alla contabilità pubblica e al nuovo Codice dei Contratti.

Formatore accreditato in ambito scolastico, collabora con enti come INDIRE, Eurosofia, Academy – Gruppo editoriale La Scuola e Il Capitello, e con diverse scuole polo per la formazione del personale ATA.

Dal 2015 si occupa di formazione del personale ATA in tutta Italia con particolare riferimento ai profili di Collaboratore Scolastico, Assistente Amm.vo e Tecnico

Abstract

"La password dimenticata" – Un caso di gestione scorretta delle credenziali informatiche.
Il caso descrive una situazione all'interno di un istituto scolastico, in cui un collaboratore condivide impropriamente le proprie credenziali di accesso al computer con un collega che ha dimenticato le sue. L'episodio mette in luce come agire per la gestione delle utenze informatiche ed i rischi connessi alla violazione delle regole base di sicurezza e privacy.

Scenario

M., collaboratrice scolastica in servizio presso la sede centrale di un istituto comprensivo, utilizza quotidianamente il PC della portineria per svolgere alcune attività digitali. Un giorno arriva G., collega di un altro plesso, che ha bisogno di usare il computer, ma non ricorda le sue credenziali: chiede quindi a M. di usare il suo account. Lei accetta, lo fa accedere e si allontana. G. consulta dei documenti, ma lascia involontariamente l'account aperto e accessibile. Il sistema viene quindi esposto a rischi di sicurezza e violazione della privacy.

Obiettivi formativi

Gli obiettivi formativi di questo caso sono i seguenti:

- Sottolineare l'importanza di utilizzare esclusivamente le **proprie credenziali personali**.
- Evidenziare i **rischi legati alla condivisione di utenze** e password.
- Promuovere comportamenti corretti in caso di **dimenticanza delle credenziali**

Contesto

Il caso si svolge in istituto comprensivo, nel plesso in cui è presente la portineria con un PC al quale accedono i collaboratori scolastici per le attività quotidiane.

Un giorno un collega chiede di accedere al PC utilizzando non le proprie credenziali, ma quelle della collega in servizio. L'accesso viene effettuato e, per errore, alcuni documenti restano aperti sul desktop.
In questo modo, si generano pericolose conseguenze per la protezione del dispositivo stesso e per la salvaguardia dei dati in esso salvati.

Problema di partenza

Alla portineria della sede centrale di un Istituto comprensivo, la collaboratrice scolastica M. accede al PC utilizzando le proprie credenziali personali per la gestione delle attività quotidiane di competenza.
Mentre sta lavorando, si rende conto che sta visualizzando documenti riservati del personale lasciati aperti sul desktop.
A seguito di un corso già svolto la collaboratrice si accorge che alcuni documenti privati sono rimasti del tutto visibili: procede con la segnalazione all'assistente tecnico, che riconosce una violazione delle procedure di sicurezza.

Strategie e strumenti

Ecco un elenco di strategie e strumenti che il collaboratore scolastico può adottare in situazioni simili a quella descritta nel caso pratico, per garantire la sicurezza informatica e il rispetto della privacy.
In primo luogo, è fondamentale utilizzare esclusivamente le proprie credenziali personali: ciascun collaboratore deve accedere al computer con il proprio nome utente e password, assegnati individualmente.
Anche in caso di urgenze o colleghi fidati, non cedere mai alla richiesta di usare le proprie credenziali: è un comportamento vietato e pericoloso; se un collaboratore dimentica le credenziali, deve rivolgersi direttamente all'assistente tecnico o al referente designato per il recupero.
Quando si lascia il computer, anche solo per pochi minuti, è essenziale eseguire il logout per evitare accessi non autorizzati. In caso di accessi sospetti, documenti aperti o account lasciati attivi da altri, occorre informare immediatamente l'assistente tecnico, o il DSGA.

Articolazione delle attività

Per quanto riguarda le attività che il collaboratore scolastico può adottare per affrontare correttamente il caso presentato, occorre ricordare quali sono i comportamenti responsabili nella gestione di imprevisti digitali, al fine di contribuire alla sicurezza dell'ambiente informatico, secondo le buone pratiche in materia di sicurezza informatica e protezione dei dati personali.
Per la corretta protezione dei dispositivi digitali, il collaboratore deve disconnettersi sempre dal proprio account prima di lasciare incustodito il computer. In caso di brevi assenze, è bene bloccare lo schermo. In questo modo, eviterà l'accesso a persone non autorizzate.
Nell'ambito della protezione dei dati personali e della privacy, è necessario utilizzare esclusivamente le proprie credenziali personali di accesso e non condividere username e password con nessuno. In caso di dimenticanza delle credenziali, sarà necessario contattare l'assistente tecnico, non chiedere ai colleghi.
Infine, per garantire la sicurezza nell'uso delle tecnologie digitali, occorre riconoscere i rischi derivanti dall'accesso non autorizzato (es. esposizione a dati sensibili o modifiche involontarie); nel

caso, segnalare immediatamente eventuali accessi anomali o sospetti all'assistente tecnico o al DSGA.

Bibliografia

- AgID. (2022). *Linee guida per la sicurezza ICT nelle pubbliche amministrazioni*. Agenzia per l'Italia Digitale.
- Autorità Garante per la Protezione dei Dati Personali. (2021). *Scuola e privacy: vademecum*.
- Calzolari, A. (2021). *Privacy e digitale: come proteggere i dati nella scuola*. Torino: Edizioni Didattiche Gulliver.
- Cert-AgID. (2023). *Rapporto annuale sulla sicurezza informatica nella PA*.
- CNIL & MIUR. (2020). *Guida alla sicurezza per gli operatori scolastici*. Trad. italiana, Commissione Europea.
- Ferraris, P. (2021). *Cybersecurity nella scuola: proteggere dati e dispositivi*. Milano: Guerini.
- Garlati, R. (2020). *Protezione dei dati personali e sicurezza informatica nella scuola*. Roma: Maggioli Editore.
- Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione. (2023). *Buone pratiche di sicurezza informatica per le scuole*.
- MIUR. (2020). *Linee guida per l'educazione civica digitale nelle scuole*.
- Poli, C. (2019). *Sicurezza informatica: guida per gli enti pubblici*. Bologna: Il Mulino.